IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Dirk Wertenbruch, et al	)	Confirmation No.: 3449
	)	
Application Serial No.: 10/664,264	)	Examiner: Ellen C. Tran
	)	
Filing Date: September 16, 2003	)	Art Unit: 2134

For: METHOD AND APPARATUS FOR CONFIGURING NETWORK DEVICES

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed on December 6, 2007.

I. REAL PARTY IN INTEREST

Cisco Systems, Inc. of San Jose, California is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

The Appellants are unaware of any related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-41 have been finally rejected and are the only subjects of this appeal.

IV. STATUS OF AMENDMENTS

The claims were not amended after the Final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application contains six independent claims: Claims 1, 10, 14, 15, 24, and 33. Claims 1, 10, 14, 15, 24, and 33 are summarized below and annotated to cross-reference features of that claim to specific examples of those features disclosed in the specification. However, the annotations are not intended to limit the scope of the recited features to those specific examples to which the annotations refer.

The claims solve the problem, for example, of how a network service provider is to identify and authenticate a network device in a network when the network service provider does not directly control the network device. For example, the network service provider might ship an ADSL interface adapter or modem to a residential broadband customer, who plugs the adapter or modem into an ADSL line in the residence. The network service provider needs to provide the adapter or modem with a unique identifier, and hard-wiring an identifier into the unit is undesirable; the network service provider also needs to authenticate the network device to prevent piracy or the use of unauthorized devices. When the adapter or modem performs data communication using a primary signaling technology and a secondary signaling technology together (such as ADSL or ISDN, for example, which is commonly used in Europe and other markets), the secondary signaling technology may inherently provide a unique identifier that can be obtained and used as a unique device identifier, although not intended for that purpose. For example, the adapter or modem can automatically obtain an ISDN link identifier that is established by a telecommunications carrier, adopt that link identifier as a unique device identifier, and notify the network service provider over the primary signaling technology that the identifier was adopted and provides its value.

Claim 1 recites *(with added reference annotations in parenthesis)* a method of authenticating a network device, comprising the computer-implemented steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device *(page 8 lines 16-17; page 11 lines 18-20; FIG. 3A ref. 304)*;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology *(page 8 lines 17-18; page 14 lines 16-19; FIG. 2 ref. 206; FIG. 3A ref. 306)*;

establishing the unique link identifier as a unique device identifier *(page 8 lines 18-19; page 11 line 1; FIG. 2 ref. 208; FIG. 3A ref. 308)*; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology *(page 8 lines 20-22; page 16 lines 12-13; page 17 lines 14-15; FIG. 2 ref. 212; FIG. 3A ref. 312);* .

Claim 10 recites *(with added reference annotations in parenthesis)* a method of authenticating a broadband customer premises network device *(page 9 line 18)* that is communicatively coupled to an ISDN line that supports ADSL over ISDN *(page 10 lines 7-8; FIG. 3B ref. 324)*, the method comprising the computer-implemented steps of:

obtaining, using the ISDN line, an ISDN telephone number uniquely associated with the ISDN line *(page 10 lines 9-10; page 11 lines 20-22; page 13 lines 4-5; page 14 lines 22-24; FIG. 3B ref 326)*;

establishing the ISDN telephone number as a unique identifier of the broadband customer premises network device *(page 10 lines 10-11; FIG. 3B ref. 328)*; and

authenticating the network device to a broadband network service provider by providing the unique identifier to the service provider using ADSL communication over the ISDN line *(page 10 lines 11-12; FIG. 3B ref. 332).*

Claim 14 recites *(with added reference annotations in parenthesis)* a method of deploying a network device *(page 10 line 19)*, comprising the steps of:

receiving a customer premises equipment (CPE) device at a customer premises *(page 10 lines 20-22)*;

coupling a network link that supports a primary signaling technology and a secondary signaling technology to the network device *(page 10 lines 22-23)*;

obtaining, using the secondary signaling technology, a unique link identifier associated with the network link *(page 10 lines 23-24)*;

establishing the unique link identifier as a unique identifier of the CPE device *(page 11 line 1)*;

connecting to a network service provider using the primary signaling technology *(page 11 lines 1-2)*;

authenticating the CPE device to a service provider by providing the unique device identifier over the network link using the primary signaling technology *(page 11 lines 2-4)*; and

receiving, from the service provider, a configuration for the CPE device over the network link *(page 11 lines 4-5)*.

Claim 15 recites *(with added reference annotations in parenthesis)* a computer-readable medium *(page 25 lines 6-7)* carrying one or more sequences of instructions for authenticating a network device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device *(page 8 lines 16-17; page 11 lines 18-20; FIG. 3A ref. 304)*;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology *(page 8 lines 17-18; page 14 lines 16-19; FIG. 2 ref. 206; FIG. 3A ref. 306)*;

establishing the unique link identifier as a unique device identifier *(page 8 lines 18-19; page 11 line 1; FIG. 2 ref. 208; FIG. 3A ref. 308)*; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology *(page 8 lines 20-22; page 16 lines 12-13; page 17 lines 14-15; FIG. 2 ref. 212; FIG. 3A ref. 312)*.

Claim 24 recites *(with added reference annotations in parenthesis)* an apparatus for configuring a network device *(page 24 lines 21-22)*, comprising:

means for determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device *(page 8 lines 16-17; page 11 lines 18-20; FIG. 3A ref. 304)*;

means for obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology *(page 8 lines 17-18; page 14 lines 16-19; FIG. 2 ref. 206; FIG. 3A ref. 306)*;

means for establishing the unique link identifier as a unique device identifier *(page 8 lines 18-19; page 11 line 1; FIG. 2 ref. 208; FIG. 3A ref. 308)*; and

means for authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology *(page 8 lines 20-22; page 16 lines 12-13; page 17 lines 14-15; FIG. 2 ref. 212; FIG. 3A ref. 312).*

Claim 33 recites *(with added reference annotations in parenthesis)* an apparatus for configuring a network device, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom *(page 11 lines 19-21)*;

a processor *(page 24 line 22)*;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device *(page 8 lines 16-17; page 11 lines 18-20; FIG. 3A ref. 304)*;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology *(page 8 lines 17-18; page 14 lines 16-19; FIG. 2 ref. 206; FIG. 3A ref. 306)*;

establishing the unique link identifier as a unique device identifier *(page 8 lines*

18-19; page 11 line 1; FIG. 2 ref. 208; FIG. 3A ref. 308); and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology *(page 8 lines 20-22; page 16 lines 12-13; page 17 lines 14-15; FIG. 2 ref. 212; FIG. 3A ref. 312).*

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-41 stand rejected under 35 USC § 103(a) as allegedly unpatentable over Li (U.S. Pat. 6,012,088, hereinafter "*Li*") in view of Fijolek (U.S. Pat. No. 6,351,773, hereinafter "*Fijolek*").

VII. ARGUMENT

As shall be explained below, each pending claim recites at least one feature that is not taught or suggested by *Li* or *Fijolek*, either individually or in combination.

A. Features of Claims 1-9 and 14-41 Are Not Taught or Suggested by *Li* or *Fijolek*

Independent Claim 1 recites:

A method of authenticating a network device, comprising the computer-implemented steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;

establishing the unique link identifier as a unique device identifier; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology.

(Emphasis added.) Claim 1 recites the step of "obtaining, using the secondary signaling

technology, a unique link identifier that is associated with the network link using the secondary signaling technology". In other words, in this step, a link identifier that is unique to a network link that uses a primary signaling technology and a secondary signaling technology is obtained through the use of the secondary signaling technology.

This step is not taught or suggested by the *Li* reference. While *Li* shows an Internet access device that has two physical interfaces, *Li* does not teach obtaining a unique link identifier associated with one of these two physical interfaces. Indeed, the Examiner has admitted in the Final Office Action dated August 6, 2007 that "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology" is not taught in the *Li* reference.

Nonetheless, in the same Final Office Action, the Examiner referred to a telephone number in *Li* as a "unique link identifier". However, *Li* actually teaches that this is "the local telephone number of a network access server located on the ISP's network," which the user dials to connect with the ISP. (*Li* col. 11 ln. 56-60.) The telephone number is associated with the ISP, not with the user's network link. Furthermore, this telephone number cannot be unique to the user's network link, since presumably many users will be dialing the same telephone number for accessing the ISP.

In sum, *Li* does not teach or suggest the step in Claim 1 of "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology".

This step is also not taught or suggested in *Fijolek* or a combination of *Fijolek* with *Li*. *Fijolek* discloses a method in which a network device establishes a virtual connection with a third network via two uni-directional links—a downstream communications link with a first network and an upstream communications link with a second network. (*Fijolek* col. 12 ln. 13 to col. 13 ln. 3.) Significantly, *Fijolek* teaches that in order to establish this virtual connection, more than one network interface on the first network may be suitable for acting as the receiving

proxy for the network device; the choice of which one to use is arbitrary and none of the network interfaces are unique. (*Fijolek* col. 12 ln. 57-63)

The portion of *Fijolek* cited by the Examiner (*Fijolek* col. 32 ln. 8-11) as allegedly teaching "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology" merely discloses that a network device receiving a connection request from a requesting device may examine a database to see if information about the requesting device, such as a telephone number, is available. However, this disclosure does not teach obtaining a telephone number or any other unique link identifier using a secondary signaling technology. In fact, the telephone numbers mentioned in *Fijolek* are obtained from information already stored on databases (*Fijolek* col. 32 ln. 6-8).

In the Final Office Action, the Examiner responded by asserting that "Fijolek … teaches that the unique identifier can be obtained from a secondary signaling technology, such as from a database" (Final Office Action dated August 6, 2007, p. 3 ln. 9-11). The Examiner considers a database to be the claimed signaling technology, and asserts that because *Fijolek* discloses obtaining an identifier from a database, that it therefore also discloses obtaining a unique link identifier from a signaling technology. It is clear error, and not an issue of "interpreting" a reference, to contend that a database is a signaling technology. While a database stores information, a signaling technology signals, conveys and communicates information. No person of ordinary skill in the art would reasonably consider a database as a signaling technology. No person of ordinary skill in the art would reasonably consider *Fijolek* to provide the above-quoted claim feature.

Therefore, *Fijolek* also does not disclose or suggest "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology", as recited in Claim 1.

A combination of *Fijolek* with *Li* also fails to provide the recited claim feature. Such a combination would merely provide that a user could look up, in a database, the local telephone number of a network access server located on the ISP's network, which is not what is claimed.

Since neither *Li* nor *Fijolek* teaches or suggests "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology", alone or in combination, *Li* and *Fijolek* also cannot teach or suggest Claim 1's features of:

> "establishing the unique link identifier as a unique device identifier" and
>
> "authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology".

(Emphasis added.) Although the Examiner has pointed to *Li*'s teaching of using a "encrypted registration ID" as an identifier for a customer's Internet access device and authenticating the Internet access device by providing the "encrypted registration ID" to the service provider (*Li* col. 11 ln. 55 – col. 12 ln. 26), this disclosure is insufficient support for alleging that *Li* teaches the "establishing" and "authenticating" steps in Claim 1. This disclosure does not teach using a unique link identifier that is associated with the network link and that is obtained using the secondary signaling technology as a device identifier and for authentication with a service provider. In fact, the "encrypted registration ID" used in *Li* is shipped from the service provider to the customer along with the Internet access device (*Li* col. 10 ln. 66 – col. 11 ln. 1). No person of ordinary skill in the art would reasonably consider shipping as a signaling technology, and no person of ordinary skill in the art would reasonably consider *Li* to provide the above-quoted claim features.

A combination of *Fijolek* with *Li* also fails to provide the "establishing" and "authenticating" features recited in Claim 1. Such a combination would merely provide that once a customer communicates the registration ID, obtained through shipping, to the service provider,

the service provider can look up information about the customer in a database by using the registration ID, which is not what is claimed.

Since neither *Li* nor *Fijolek* teaches or suggests the features of Claim 1 discussed above, alone or in combination, Claim 1 is patentable over *Li* in view of *Fijolek* under 35 USC § 103(a).

Claims 2-9 and 14-41 either depend from Claim 1 or recite features similar to the features of Claim 1 discussed above. Consequently, it is respectfully submitted that Claims 2-9 and 14-41 are also patentable over *Li* in view of *Fijolek* for at least the reasons set forth herein with respect to Claim 1.

The rejections of Claims 1-9 and 14-41 should be reversed.

B. Features of Claims 10-13 Are Not Taught or Suggested by *Li* or *Fijolek*

Independent Claim 10 recites:

> A method of authenticating a broadband customer premises network device that is communicatively coupled to an ISDN line that supports ADSL over ISDN, the method comprising the computer-implemented steps of:
>
> obtaining, using the ISDN line, an ISDN telephone number uniquely associated with the ISDN line;
>
> establishing the ISDN telephone number as a unique identifier of the broadband customer premises network device; and
>
> authenticating the network device to a broadband network service provider by providing the unique identifier to the service provider using ADSL communication over the ISDN line.

Independent Claim 10 is patentable over *Li* and *Fijolek* for at least the reasons set forth herein with respect to independent Claim 1 because *Li* and *Fijolek* do not teach "obtaining, using the ISDN line, an ISDN telephone number uniquely associated with the ISDN line", recited in Claim 10, for the same reasons discussed above regarding *Li* and *Fijolek* not teaching "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology", recited in Claim 1. Although *Li* mentions both

ADSL and ISDN signaling technologies in general (*Li* col. 3 ln. 46-43 and col. 7 ln. 3-11), neither *Li* nor *Fijolek* teaches the step of "obtaining, using the ISDN line, an ISDN telephone number uniquely associated with the ISDN line" in Claim 10.

A combination of *Fijolek* with *Li* also fails to provide the recited claim feature. Such a combination would merely provide that a user could look up, in a database, an ISDN line number of a network access server located on the ISP's network, which is not what is claimed.

Li and *Fijolek* also do not teach or suggest the features of "establishing the ISDN telephone number as a unique identifier of the broadband customer premises network device" and "authenticating the network device to a broadband network service provider by providing the unique identifier to the service provider using ADSL communication over the ISDN line" for the reasons that are stated above with respect to the "establishing" and "authenticating" features of Claim 1.

Thus, Claim 10 is patentable over *Li* in view of *Fijolek* under 35 USC § 103(a).

Claims 11-13 depend from Claim 10. Consequently, it is respectfully submitted that Claims 11-13 are also patentable over *Li* in view of *Fijolek* for at least the reasons set forth herein with respect to Claim 10.

The rejections of Claims 10-13 should be reversed.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the reasons set forth above, it is respectfully submitted that the rejections of Claims 1-41 lack the requisite factual and legal bases. Appellants respectfully request that the Honorable Board reverse the rejections of Claims 1-41.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

/YipingRLiao#60301/
Yiping R. Liao
Reg. No. 60,301

Date: March 12, 2008

2055 Gateway Place, Suite 550
San Jose, CA 95110
(408) 414-1080
Facsimile: (408) 414-1076

CLAIMS APPENDIX

1. A method of authenticating a network device, comprising the computer-implemented steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;

establishing the unique link identifier as a unique device identifier; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology.

2. A method as recited in Claim 1, further comprising the steps of receiving a configuration from the service provider over the network link using the primary signaling technology.

3. A method as recited in Claim 1, wherein the secondary signaling technology is integrated services digital network (ISDN) signaling.

4. A method as recited in Claim 1, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier is a telephone number associated with an ISDN line coupled to the network device.

5. A method as recited in Claim 1, wherein the secondary signaling technology is ISDN, and

wherein the obtaining step comprises obtaining a telephone number associated with an ISDN line coupled to the network device using a caller ID function.

6. A method as recited in Claim 1, wherein the network device is a residential broadband router, wherein the primary signaling technology is asynchronous digital subscriber line (ADSL), and wherein the secondary signaling technology is ISDN.

7. A method as recited in Claim 1, wherein the network device is a residential broadband router, wherein the primary signaling technology is ADSL, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier is a telephone number associated with an ISDN line.

8. A method as recited in Claim 7, wherein the step of registering the network device with a service provider comprises using the ADSL line to connect to a Cisco Intelligent Engine 2100 (IE2100) device associated with the service provider, and providing the unique device identifier to the IE2100.

9. A method as recited in Claim 1, wherein the step of registering the network device with a service provider comprises using the primary signaling technology to connect to a configuration server associated with the service provider, and providing the unique device identifier to the configuration server.

10. A method of authenticating a broadband customer premises network device that is

communicatively coupled to an ISDN line that supports ADSL over ISDN, the method comprising the computer-implemented steps of:

obtaining, using the ISDN line, an ISDN telephone number uniquely associated with the ISDN line;

establishing the ISDN telephone number as a unique identifier of the broadband customer premises network device; and

authenticating the network device to a broadband network service provider by providing the unique identifier to the service provider using ADSL communication over the ISDN line.

11. A method as recited in Claim 10, further comprising the steps of receiving a configuration from the service provider.

12. A method as recited in Claim 10, wherein the obtaining step comprises obtaining a telephone number associated with the ISDN line using a caller ID function.

13. A method as recited in Claim 10, wherein the step of registering the network device with the service provider comprises using ADSL over ISDN to connect to a Cisco Intelligent Engine 2100 (IE2100) device associated with the service provider, and providing the unique device identifier to the IE2100.

14. A method of deploying a network device, comprising the steps of:

receiving a customer premises equipment (CPE) device at a customer premises;

coupling a network link that supports a primary signaling technology and a secondary signaling technology to the network device;

obtaining, using the secondary signaling technology, a unique link identifier associated with the network link;

establishing the unique link identifier as a unique identifier of the CPE device;

connecting to a network service provider using the primary signaling technology;

authenticating the CPE device to a service provider by providing the unique device identifier over the network link using the primary signaling technology; and

receiving, from the service provider, a configuration for the CPE device over the network link.

15. A computer-readable medium carrying one or more sequences of instructions for authenticating a network device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;

establishing the unique link identifier as a unique device identifier; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology.

16. A computer-readable medium as recited in Claim 15, further comprising the steps of receiving a configuration from the service provider.

17. A computer-readable medium as recited in Claim 15, wherein the secondary signaling technology is ISDN.

18. A computer-readable medium as recited in Claim 15, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary telecommunication link is a telephone number associated with an ISDN line.

19. A computer-readable medium as recited in Claim 15, wherein the secondary signaling technology is ISDN, and wherein the obtaining step comprises obtaining a telephone number associated with an ISDN line using a caller ID function.

20. A computer-readable medium as recited in Claim 15, wherein the network device is a residential broadband router, and wherein the primary signaling technology is ADSL.

21. A computer-readable medium as recited in Claim 15, wherein the network device is a residential broadband router, wherein the primary signaling technology is ADSL, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary telecommunication link is a telephone number associated with an ISDN line.

22. A computer-readable medium as recited in Claim 21, wherein the step of registering the

network device with a service provider comprises using ADSL to connect to a Cisco Intelligent Engine 2100 (IE2100) device associated with the service provider, and providing the unique device identifier to the IE2100.

23. A computer-readable medium as recited in Claim 15, wherein the step of registering the network device with a service provider comprises using the primary signaling technology to connect to a configuration server associated with the service provider, and providing the unique device identifier to the configuration server.

24. An apparatus for configuring a network device, comprising:

means for determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;

means for obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;

means for establishing the unique link identifier as a unique device identifier; and

means for authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology.

25. An apparatus as recited in Claim 24, further comprising:

means for receiving a configuration from the service provider over the primary network link; and

means for initiating in-service operation.

26. An apparatus as recited in Claim 24, wherein the secondary signaling technology is ISDN.

27. An apparatus as recited in Claim 24, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary signaling technology is a telephone number associated with an ISDN line.

28. An apparatus as recited in Claim 24, wherein the secondary signaling technology is ISDN, and wherein the obtaining means comprises means for obtaining a telephone number associated with the ISDN line using a caller ID function.

29. An apparatus as recited in Claim 24, wherein the network device is a residential broadband router, and wherein the primary signaling technology is ADSL.

30. An apparatus as recited in Claim 24, wherein the network device is a residential broadband router, wherein the primary signaling technology is ADSL, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary signaling technology is a telephone number associated with an ISDN line.

31. An apparatus as recited in Claim 30, wherein the step of registering the network device with a service provider comprises using ADSL to connect to a Cisco Intelligent Engine 2100 (IE2100) device associated with the service provider, and providing the unique device identifier

to the IE2100.

32. An apparatus as recited in Claim 24, wherein the registering means comprises means for using the primary signaling technology to connect to a configuration server associated with the service provider, and for providing the unique device identifier to the configuration server.

33. An apparatus for configuring a network device, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor,

cause the processor to carry out the steps of:

determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;

obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;

establishing the unique link identifier as a unique device identifier; and

authenticating the network device to a service provider by communicating the unique device identifier to the service provider over the network link using the primary signaling technology.

34. An apparatus as recited in Claim 33, further comprising the steps of receiving a

configuration from the service provider.

35. An apparatus as recited in Claim 33, wherein the secondary signaling technology is ISDN.

36. An apparatus as recited in Claim 33, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary signaling technology is a telephone number associated with an ISDN line.

37. An apparatus as recited in Claim 33, wherein the secondary signaling technology is ISDN, and wherein the obtaining step comprises obtaining a telephone number associated with an ISDN line using a caller ID function.

38. An apparatus as recited in Claim 33, wherein the network device is a residential broadband router, and wherein the primary signaling technology is ADSL.

39. An apparatus as recited in Claim 33, wherein the network device is a residential broadband router, wherein the primary signaling technology is ADSL, wherein the secondary signaling technology is ISDN, and wherein the unique link identifier associated with the secondary signaling technology is a telephone number associated with an ISDN line.

40. An apparatus as recited in Claim 33, wherein the step of registering the network device with a service provider comprises using the ADSL line to connect to a Cisco Intelligent Engine

2100 (IE2100) device associated with the service provider, and providing the unique device identifier to the IE2100.

41. An apparatus as recited in Claim 33, wherein the step of registering the network device with a service provider comprises using the primary signaling technology to connect to a configuration server associated with the service provider, and providing the unique device identifier to the configuration server.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.